

REENA RAGGI, *Circuit Judge*, joined by DENNIS JACOBS, JOSÉ A. CABRANES, and CHRISTOPHER F. DRONEY, *Circuit Judges*, dissenting from the order denying rehearing *en banc*:

In this case, a panel of the court quashes a compelled-disclosure warrant issued under the Stored Communications Act (“SCA”) by a neutral magistrate and supported by probable cause to think that the information demanded is evidence of a crime. *See* 18 U.S.C. § 2703(a). The ground for decision is the presumption against extraterritoriality, *see Morrison v. Nat’l Australia Bank Ltd.*, 561 U.S. 247, 255 (2010), which the panel construes to allow United States corporation Microsoft to refuse to disclose subscriber communications in its possession and responsive to the warrant because Microsoft, for its own business reasons and unbeknownst to its subscriber, has chosen to store the communications in Ireland. The panel does not simply set a *higher* bar for the government to secure such electronic communications. Rather, it erects an “*absolute*” bar so that “the government can never obtain a warrant that would require Microsoft,” or any other U.S.-based service provider, to turn over electronic communications stored abroad, “however certain it may be that they contain evidence of criminal activity, and even if that criminal activity is a

terrorist plot.” *Microsoft Corp. v. United States* (“*Microsoft*”), 829 F.3d 197, 224 (2d Cir. 2016) (Lynch, J., concurring in the judgment) (emphasis in original).¹ This ruling merits *en banc* review. To the extent an equally divided court today denies such review, I respectfully dissent.

1. Matter of Exceptional Importance

The panel’s ruling, the reasoning informing it, and its disturbing consequences raise questions “of exceptional importance to public safety and national security.” Cabranes, J., Op. Dissenting from Denial of Reh’g En Banc (“Cabranes, J., Op.”), *ante* at 1. The panel nevertheless urges us to forego *en banc* review because the SCA is outdated and overdue for congressional revision. *See Microsoft*, 829 F.3d at 201; Carney, J., Op. Concurring in Denial of Reh’g En Banc (“Carney, J., Op.”), *ante* at 2 & n.3. I am not persuaded.

This is not a case where some legal principle (*e.g.*, standing, mootness) allowed the panel to avoid applying the SCA, thereby affording Congress time to enact new legislation. This is a case where the panel reached the merits and

¹ On the panel’s reasoning, if on September 10, 2001, the government had been able to show probable cause to believe that Mohamed Atta, Abdul Aziz al Omari, etc., were communicating electronically about an imminent, devastating attack on the United States, and that Microsoft possessed those emails, no federal court could have issued a § 2703(a) warrant compelling Microsoft to disclose those emails if it had stored them overseas, even though its employees would not have had to leave their desks in Redmond, Washington, to retrieve them.

construed the SCA to foreclose altogether § 2703(a) warrants requiring United States service providers to disclose electronic communications stored overseas. This construction now controls the SCA's application in this circuit. In its Petition for Rehearing, the government details the immediate and serious adverse consequences of such a ruling. *See* Gov't Pet. for Reh'g at 18–19; *see also* Cabranes, J., Op., *ante* at 2–7. These consequences cannot be attributed to deficiencies in the SCA. Rather, they derive from the panel's conclusion—mistaken in my view—that the SCA is impermissibly being applied extraterritorially when a § 2703(a) warrant requires a United States service provider to disclose electronic communications that it has elected to store abroad. It is simply unprecedented to conclude that the presumption against extraterritoriality bars United States courts with personal jurisdiction over a United States person from ordering that person to produce property in his possession (wherever located) when the government has made a probable cause showing that the property is evidence of a crime. This alone warrants *en banc* review.

2. The Panel's Discussion of "Warrant"

Several aspects of the panel's extraterritoriality analysis require particular review. The first is the panel's lengthy discussion of why Congress's "use of the term of art 'warrant'" in the SCA manifests an intent for the statute to operate only domestically. *Microsoft*, 829 F.3d at 212. At the outset, I note that there was no need for the panel to locate *domestic* intent in the SCA; it is presumed in the absence of a showing of express *extraterritorial* intent, which the government concedes is absent here. *See Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. at 255. The panel majority's "warrant" discussion, however, is not simply unnecessary. It is also flawed in ways that lay an unsound foundation for the panel's ensuing identification of statutory "focus."

Notably, the panel majority concludes that Congress's use of the term "warrant" in § 2703 signals its intent to invoke all of the "traditional, domestic connotations" that pertain to traditional search warrants. *Microsoft*, 829 F.3d at 213. But, as Judge Lynch observes, a § 2703(a) warrant is not a traditional warrant. *Id.* at 226 (Lynch, J., concurring in the judgment). It does not authorize federal agents to *search* any premises or to *seize* any person or materials. Rather, it authorizes a federal agent to require a service provider to disclose materials in

its possession. The difference is significant to identifying where a warrant is being executed. Because a search warrant is executed with respect to a *place*—the place to be searched—the presumption against extraterritoriality expects that place to be within United States territory. By contrast, because a § 2703(a) warrant is executed with respect to a *person*—the person ordered to divulge materials in his possession—the presumption against extraterritoriality expects that person to be within United States territory and subject to the court’s jurisdiction. If the person is so present, execution of the warrant as to him is a domestic application of United States law without regard to from where the person must retrieve the materials ordered disclosed. Indeed, if that were not so, subpoenas requiring persons in this country to produce materials that they must retrieve from abroad could not be enforced, a position contrary to well established law. *See, e.g., Marc Rich & Co., A.G. v. United States*, 707 F.2d 663, 668–70 (2d Cir. 1983); *United States v. Bank of Nova Scotia (In re Grand Jury Proceedings)*, 740 F.2d 817, 826–29 (11th Cir. 1984).

Thus, I respectfully submit that the panel majority’s extraterritoriality analysis starts with the mistaken equation of § 2703(a) warrants with traditional

search warrants. This, in turn, leads to the mistaken conclusion that “a warrant protects privacy in a distinctly territorial way.” *Microsoft*, 829 F.3d at 212.

As to the latter point, the reason United States search warrants do not apply extraterritorially has to do with *sovereignty*, not *privacy*. Since before the republic, the law of nations has recognized that one sovereign cannot unilaterally enforce its criminal laws within the territory of another.² But a defendant’s expectations of privacy do not preclude evidence so obtained from being used in a United States prosecution. See *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 176–77 (2d Cir. 2008). Thus, it is respect for sovereign independence that has prompted us to observe that “search warrants intended to have extraterritorial effect . . . would have dubious legal significance, if any, in a foreign nation.” *Id.* at 171. But this observation, quoted by the panel majority, does not support its ensuing conclusion that, “[a]ccordingly, a warrant protects

² See Restatement (Third) of Foreign Relations Law § 432(2) (“A state’s law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state.”); 1 *Oppenheim’s International Law* § 119 (Robert Jennings & Arthur Watts, eds., 9th ed. 1992) (“It is . . . a breach of international law for a state without permission to send its agents into the territory of another state to apprehend persons accused of having committed a crime.”); *The Apollon*, 22 U.S. (9 Wheat.) 362, 371 (1824) (Story, J.) (holding that “[i]t would be monstrous to suppose that our revenue officers were authorized to enter into foreign ports and territories, for the purpose of seizing vessels which had offended against our laws” because such conduct would be “a clear violation of the laws of nations”); *The Nereide*, 13 U.S. (9 Cranch) 388, 423 (1815) (Marshall, C.J.) (“[T]he Court is bound by the law of nations which is a part of the law of the land.”).

privacy in a distinctly territorial way.” *Microsoft*, 829 F.3d at 212 (emphasis added).

As Judge Lynch explains, how warrants protect *privacy* is through the Fourth Amendment requirement that they issue only “upon probable cause.” U.S. Const. amend. IV; *see Microsoft*, 829 F.3d at 223 (Lynch, J., concurring in the judgment). Indeed, to the extent the SCA’s legislative history shows Congress’s intent to extend privacy protections, specifically, protections “analogous to those provided by the Fourth Amendment,” to certain electronic communications, *Microsoft*, 829 F.3d at 206 (quoting Gov’t Br. at 29), one might better understand Congress to have used the term “warrant” in § 2703(a) to ensure that certain disclosures would be compelled only upon a showing of probable cause. Thus, when a § 2703(a) warrant supported by probable cause is executed on a person within the jurisdiction of the United States, the SCA is being applied domestically without regard to the location of the materials that the person must divulge.

As Judge Cabranes observes, by failing to recognize these distinctions (a) between search warrants directed to particular locations and § 2703(a) warrants directed to particular persons, and (b) between the values of sovereignty and

privacy, the panel majority construes “warrant” as used in § 2703 to yield a perverse result: affording *greater* privacy protection to foreign citizens and Americans who claim to reside abroad than to resident U.S. citizens. *See Cabranes, J., Op., ante* at 7–8 n.19. This troubling result and the reasons leading to it warrant *en banc* review.

3. The Focus of the Statute

Where, as here, the government does not argue that Congress intended for § 2703(a) to apply extraterritorially, the determinative question asks whether the domestic contacts associated with that statutory provision are sufficient to avoid triggering the presumption against extraterritoriality. To answer that question, a court looks to “the territorial events or relationships” that are the “focus” of the relevant statutory provision. *Mastafa v. Chevron Corp.*, 770 F.3d 170, 184 (2d Cir. 2014) (alterations omitted); *Morrison v. Nat’l Australia Bank Ltd.*, 561 U.S. at 266–68. The panel majority identifies “privacy” as the focus of § 2703(a)’s warrant requirement. *Microsoft*, 829 F.3d at 217. It then reasons that because the § 2703(a) warrant here sought disclosure of the electronic communications of a Microsoft customer, and because Microsoft stored those communications in Dublin, “[t]he content to be *seized* is stored in Dublin.” *Id.* at 220 (emphasis added). This in

turn leads it to conclude that “the invasion of the customer’s privacy takes place under the SCA where the customer’s protected content is accessed—here, where it is *seized by Microsoft, acting as an agent of the government.*” *Id.* (emphasis added). Accordingly, it concludes that the § 2703(a) warrant is being executed in Ireland in violation of the presumption against extraterritoriality.

This reasoning raises several concerns.

First, I cannot agree that a person who is compelled by a § 2703(a) warrant to disclose to the government materials already in that person’s possession is “seiz[ing]” anything as an agent of the government. *See id.* The cases cited by the panel majority identify such agency where property is *not* already in an actor’s possession. In such circumstances, but for authorizing law or warrant, the actor could not lawfully take possession of—*i.e.*, seize—third-party materials. That is not the case here. Microsoft did not need any warrant from the United States to take possession of the subscriber communications it had stored in Ireland. Nor did it need such a warrant to transfer those communications from Ireland to the United States. Indeed, it did not need the approval of Irish authorities or even of its subscriber to take such action. Thus, it is simply wrong to characterize Microsoft’s actions in retrieving customer electronic data in

Ireland as “Microsoft’s *execution* of the warrant,” much less as a *seizure* by Microsoft. Carney, J., Op., *ante* at 3 (emphasis added); *see Microsoft*, 829 F.3d at 220. The § 2703(a) warrant here at issue was executed by *federal authorities*, who were thereby authorized to compel Microsoft to *disclose* communications already lawfully in its possession. Such disclosure by Microsoft would otherwise have been prohibited by 18 U.S.C. § 2702(a). But the only territorial event that needs to be warranted under the SCA is disclosure. No warrant was needed for Microsoft lawfully to access material on its Dublin servers from the United States. Nor is a different conclusion supported by the panel majority’s observation that our court “has never upheld the use of a subpoena to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item.” *Microsoft*, 829 F.3d at 215. The question whether the caretaker’s actions respecting materials in his possession constitute a “search” or “seizure” undertaken as an agent of the government does not turn on whether the item is located here or overseas. Indeed, as Judge Lynch states, we have upheld the use of a subpoena to compel a caretaker to produce client materials in its domestic

possession. *See id.* at 228 n.5 (Lynch, J., concurring in the judgment) (citing *In re Horowitz*, 482 F.2d 72 (2d Cir. 1973)). Such a conclusion would not have been possible if the caretaker's actions respecting materials in his possession equated to a "search" or "seizure" undertaken as an agent of the government.

Thus, we need to convene *en banc* to clarify that a service provider who complies with a § 2703(a) warrant compelling disclosure of communications in his lawful possession does not thereby conduct a search or seizure as the agent of the government.

Second, I also cannot agree with the panel that *privacy* is the focus of § 2703 and that subscriber privacy would be invaded *in Ireland* were Microsoft to access its subscriber files there. To the extent § 2702(a) generally prohibits a service provider from knowingly disclosing subscribers' electronic communications to third parties, that provision might be understood to focus on enhancing subscriber privacy. But § 2703 identifies circumstances when the government nevertheless "may require" service providers to disclose their subscribers' communications. This gives some force to the government's argument that the focus of § 2703 is compelled *disclosure*, not enhanced *privacy*. *See* Gov't Pet. for Reh'g at 11–12 (noting that focus inquiry is "provision-specific" and citing *RJR*

Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2101–11 (2016)). *But see Microsoft*, 829 F.3d at 218–19 (rejecting disclosure focus argument).

Even assuming that the enhanced privacy and compelled disclosure provisions of the SCA are two sides of the same coin, I think the panel errs in concluding that the privacy afforded by the SCA would be invaded by Microsoft's access of its own files in Dublin rather than by its subsequent disclosure of subscriber communications in the United States.

As already stated, Microsoft is entitled to access and to move subscriber communications at will, even without consulting its subscriber. Such actions by Microsoft disclose nothing to the government about the existence or content of such communications. The only privacy interest afforded by § 2702(a), however, is against such disclosure. The statute provides no privacy right against Microsoft's own handling of communications short of such disclosure. Thus, contrary to the panel, I think that, even if privacy is the focus of §§ 2702 and 2703, the territorial event that is the focus of that privacy interest is the service provider's disclosure of the subscriber communications to a third party—whether in violation of § 2702(a) or as authorized by warrant under § 2703(a). It

is where that disclosure occurs that determines whether these statutory provisions are being applied domestically or extraterritorially.

Here, there is no question that the challenged § 2703(a) warrant issued, was served on Microsoft in, and required disclosure in the United States. Thus, even if “privacy” is the statute’s “focus,” the challenged warrant here applies the statute domestically, not extraterritorially. We should say so *en banc*.

4. Concluding Observations

Two final points. As Judge Cabranes observes, and Judge Carney seems to agree, the same reasoning that leads the panel to conclude that § 2703(a) warrants cannot reach communications that Microsoft has stored in Ireland might also preclude affording § 2702(a) privacy protections to such materials. *See Cabranes, J., Op., ante* at 14 n.36; *Carney, J., Op., ante* at 7 n.6. But if § 2702(a) protections do not apply here, does the government even need a § 2703(a) warrant? Could it simply proceed by subpoena? *See Marc Rich & Co., A.G. v. United States*, 707 F.2d at 668–70; *United States v. Bank of Nova Scotia (In re Grand Jury Proceedings)*, 740 F.2d at 826–29. I think the government does need a § 2703(a) warrant because I understand both § 2702(a) protections and § 2703(a) warrants to exercise government authority domestically on persons subject to

United States jurisdiction. To the extent, however, that the panel's extraterritoriality reasoning might allow a United States service provider such as Microsoft to flout not only § 2703(a) warrants but also § 2702(a) protections simply by moving materials abroad, the need for *en banc* review is only heightened.

My second point is not unrelated. The panel concludes that, because the Congress that enacted the SCA could not have foreseen the technological context in which this case arises, the focus of the statute cannot be domestic disclosure of data that a service provider in the United States accesses from abroad. Therefore, the warrant should be quashed. It seems to me this allows the first prong of analysis—did Congress intend extraterritoriality?—to be determinative of the second—is the statute being applied extraterritorially in the case at hand? In fact, the two steps of analysis are distinct. *See Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. at 266. Whatever Congress may have foreseen about advances in electronic communications, I think, for the reasons already stated, that the SCA is being applied domestically here. The privacy protection afforded by § 2702(a) is against unauthorized *disclosure* to third parties. But a § 2703(a) warrant here specifically authorizes federal agents to compel disclosure in the United States.

Further, the party from whom such disclosure is being compelled is a United States service provider subject to the personal jurisdiction of United States courts.

In short, this is not the case hypothesized by the panel where the government might use a § 2703(a) warrant to demand communications *stored abroad* from a *foreign service provider* relating to a *foreign subscriber*. See, e.g., *Microsoft*, 829 F.3d at 231–32 (Lynch, J., concurring in the judgment); Carney, J., Op., *ante* at 8–9.

When such a case comes before us, we can certainly consider whether a court with personal jurisdiction over the foreign service provider can issue a § 2703(a) warrant compelling it to disclose in the United States communications stored abroad. But, in this case, where the warrant is directed to a United States provider over whom there is personal jurisdiction for production in the United States of specified communications on a federal magistrate’s identification of probable cause, I simply do not think we have an extraterritorial application of U.S. law.

For the foregoing reasons, this court *en banc* should enforce, not quash, the challenged § 2703(a) warrant.